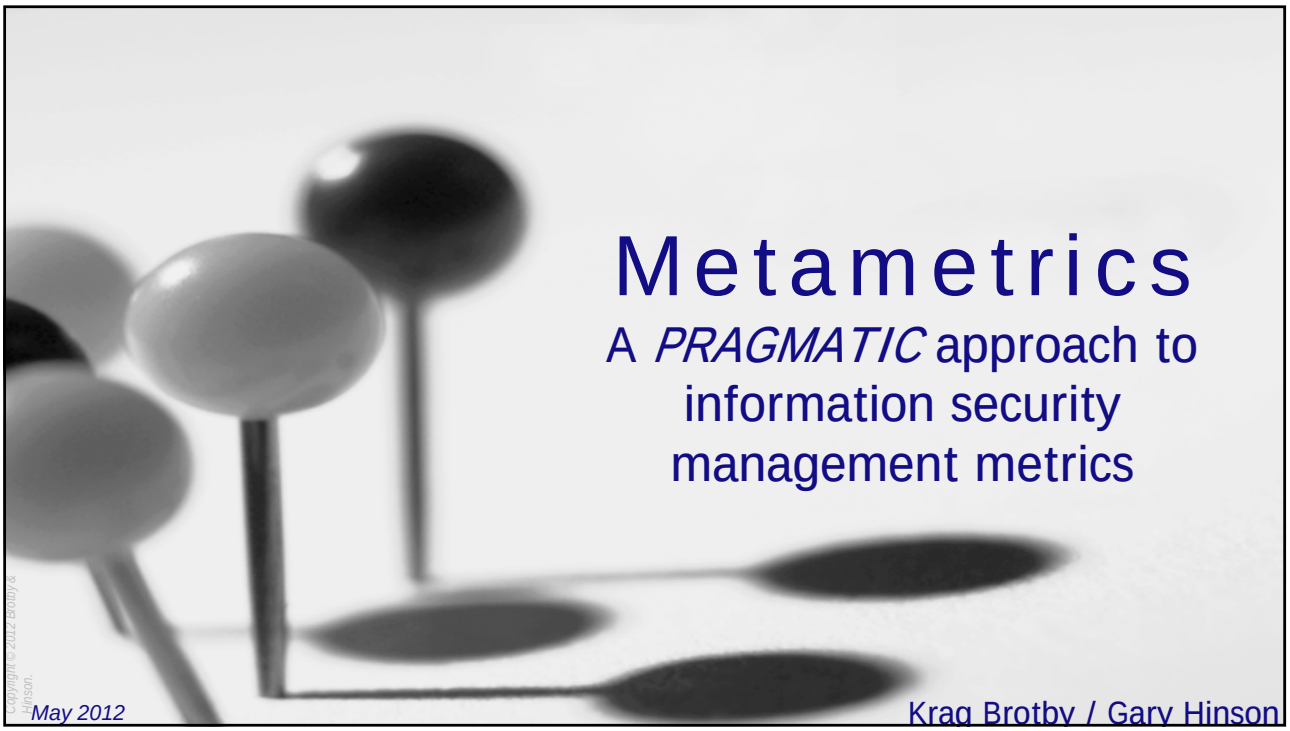
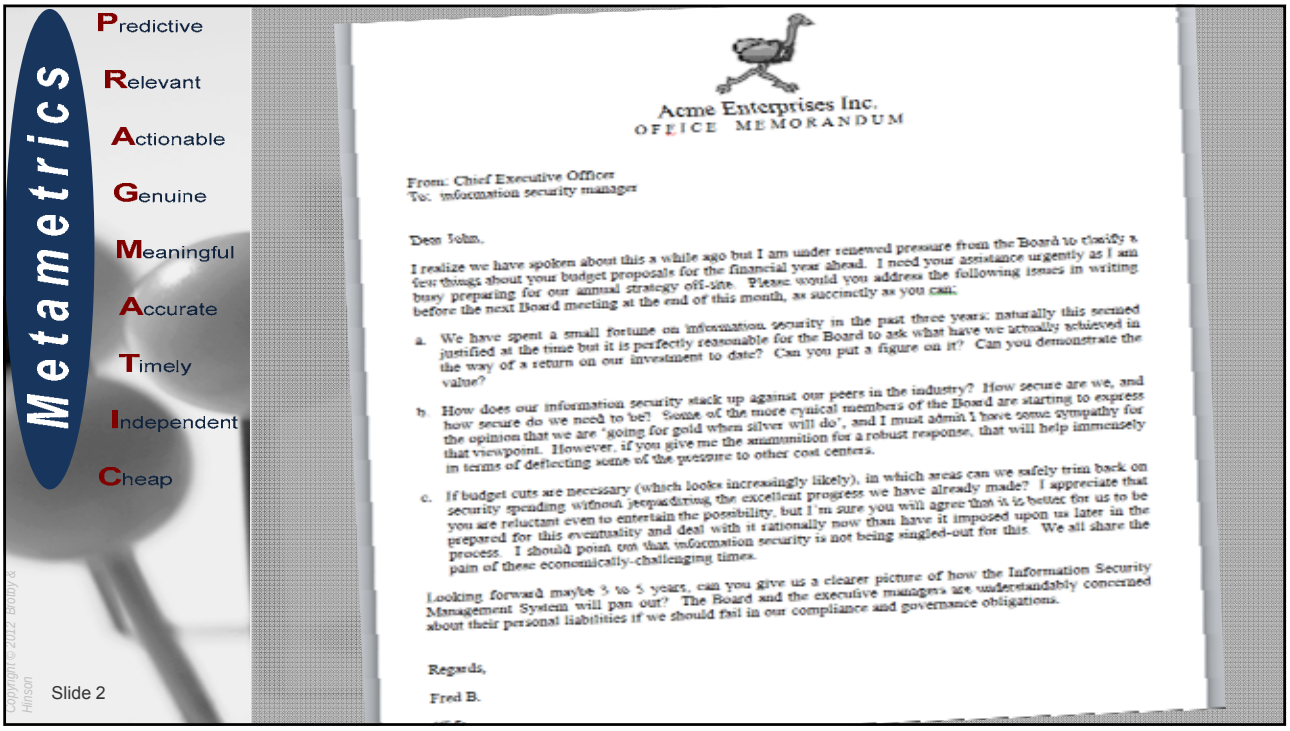


Metametrics

A *PRAGMATIC* approach to information security management metrics

May 2012

Krag Brotby / Gary Hinson



Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Why metrics?

"A man's judgment cannot be better than the information on which he has based it."

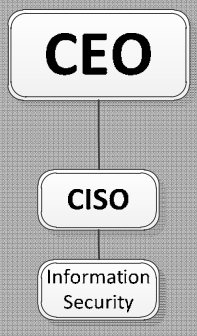
Arthur Hays Sulzberger, 1947

Slide 3

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Who are metrics for?

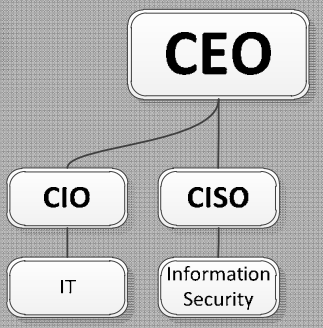


Slide 4

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Who are metrics for?



Slide 5

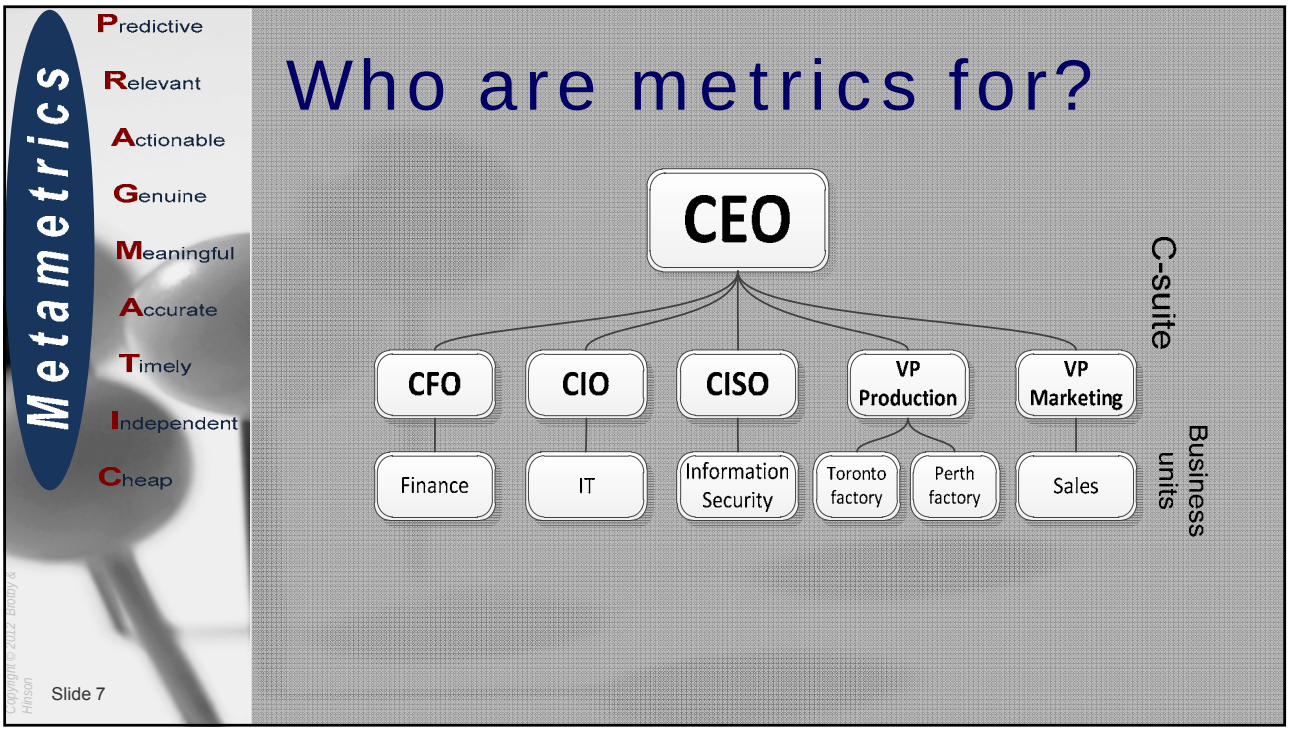
Metametrics

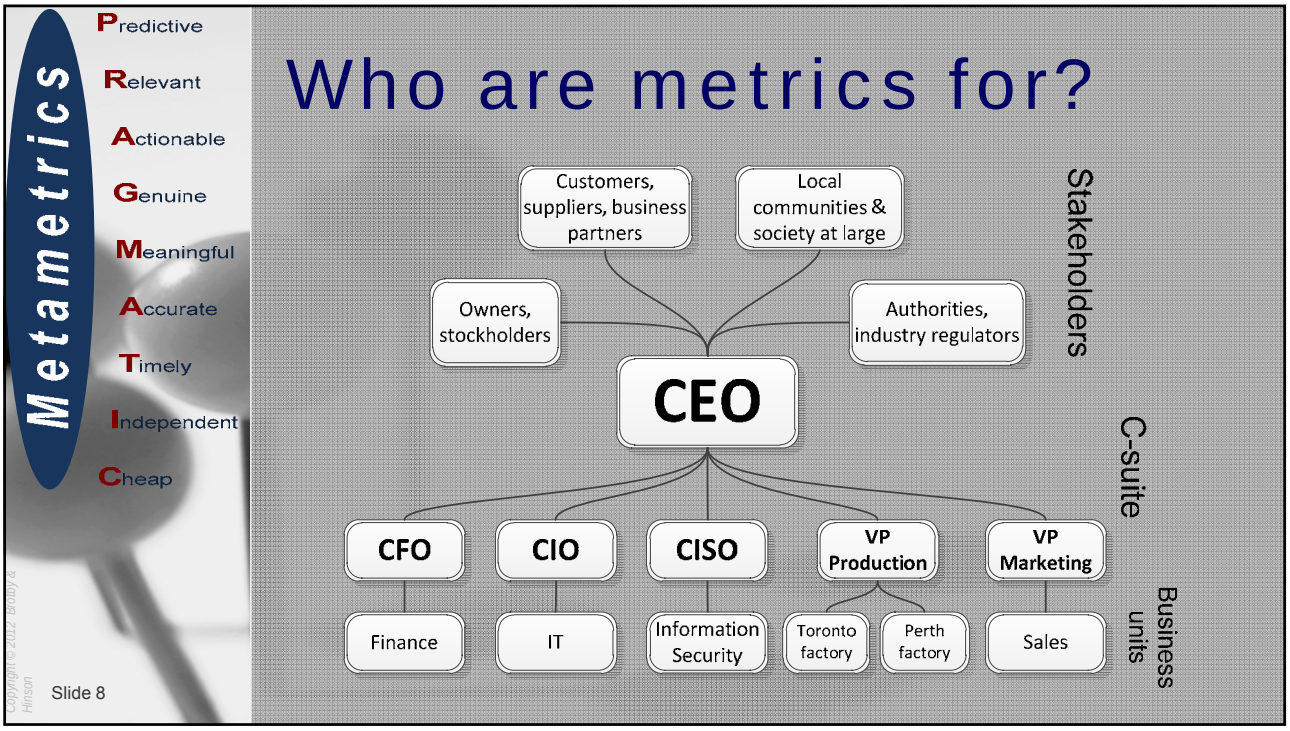
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

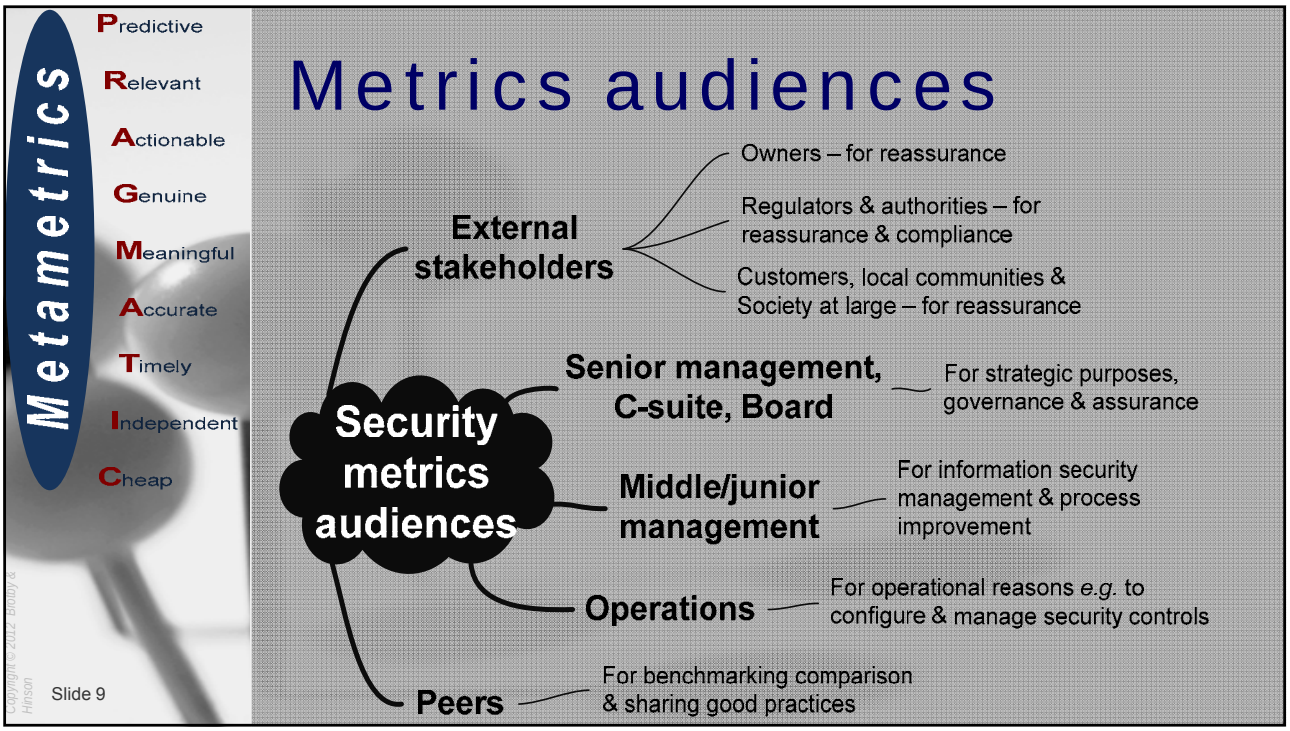
IT security metrics

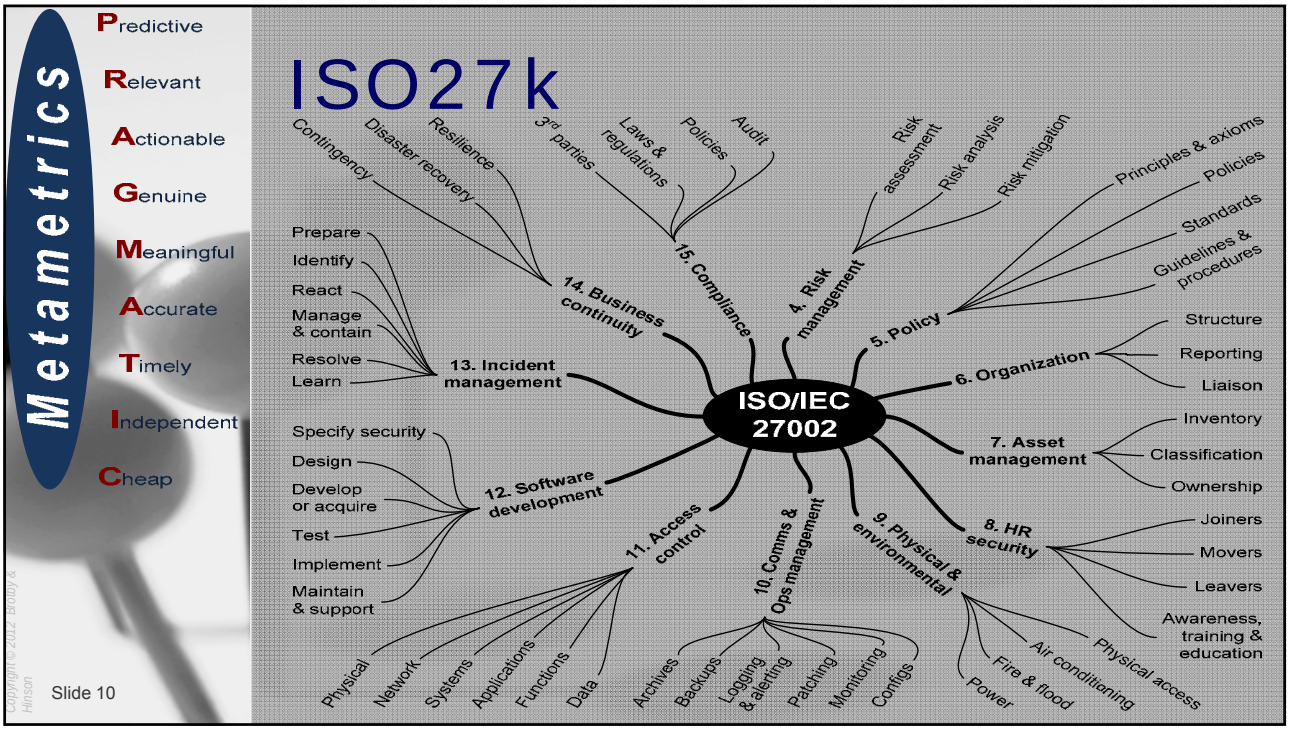
Uptime
Failed logons
Vulnerabilities identified
Malware detected
Dropped packets
Unpatched systems

Slide 6


Metametrics
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap
Who are metrics for?
CEO
CFO
CIO
CISO
VP Production
VP Marketing
Finance
IT
Information Security
Toronto factory
Perth factory
Sales
C-suite
Business units
Slide 7


Metametrics
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap
Who are metrics for?
Customers, suppliers, business partners
Local communities & society at large
Owners, stockholders
Authorities, industry regulators
Stakeholders
CEO
CFO
CIO
CISO
VP Production
VP Marketing
Finance
IT
Information Security
Toronto factory
Perth factory
Sales
C-suite
Business units
Slide 8


Metametrics
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap
Metrics audiences
Security metrics audiences
External stakeholders
Owners – for reassurance
Regulators & authorities – for reassurance & compliance
Customers, local communities & Society at large – for reassurance
Senior management, C-suite, Board
For strategic purposes, governance & assurance
Middle/junior management
For information security management & process improvement
Operations
For operational reasons e.g. to configure & manage security controls
Peers
For benchmarking comparison & sharing good practices
Slide 9


Metametrics
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap
ISO27k
ISO/IEC 27002
4. Risk management
Risk assessment
Risk analysis
Risk mitigation
5. Policy
Principles & axioms
Policies
Standards
Guidelines & procedures
6. Organization
Structure
Reporting
Liaison
7. Asset management
Inventory
Classification
Ownership
8. HR security
Joiners
Movers
Leavers
Awareness, training & education
9. Physical & environmental
Physical access
Air conditioning
Fire & flood
Power
10. Comms & Ops management
Configs
Monitoring
Patching
Logging & alerting
Backups
Archives
11. Access control
Physical
Network
Systems
Applications
Functions
Data
12. Software development
Specify security
Design
Develop or acquire
Test
Implement
Maintain & support
13. Incident management
Prepare
Identify
React
Manage & contain
Resolve
Learn
14. Business continuity
Contingency
Disaster recovery
Resilience
15. Compliance
3rd parties
Laws & regulations
Policies
Audit
Slide 10

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Goals & outcomes

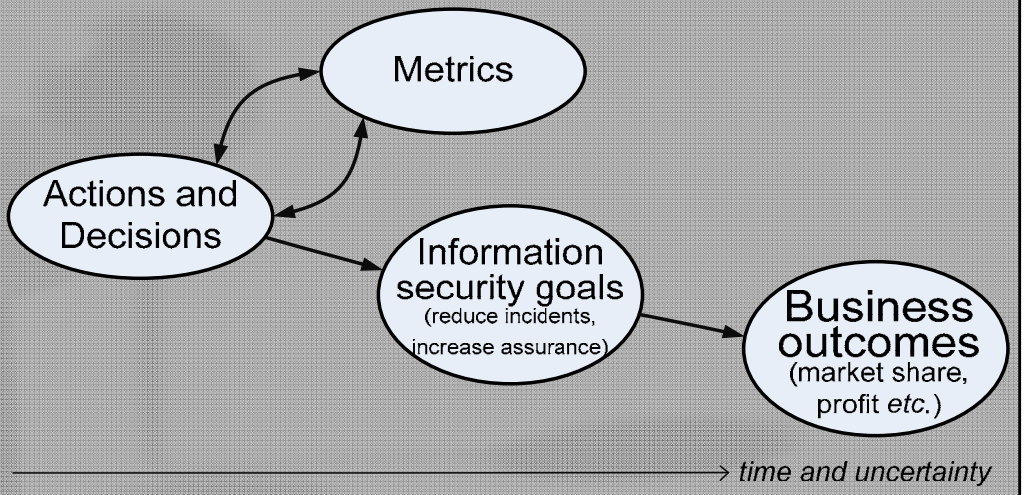


Figure adapted from Hauser and Katz *Metrics: You Are What You Measure*
www.mit.edu/~hauser/Papers/Hauser-Katz Measure 04-98.pdf

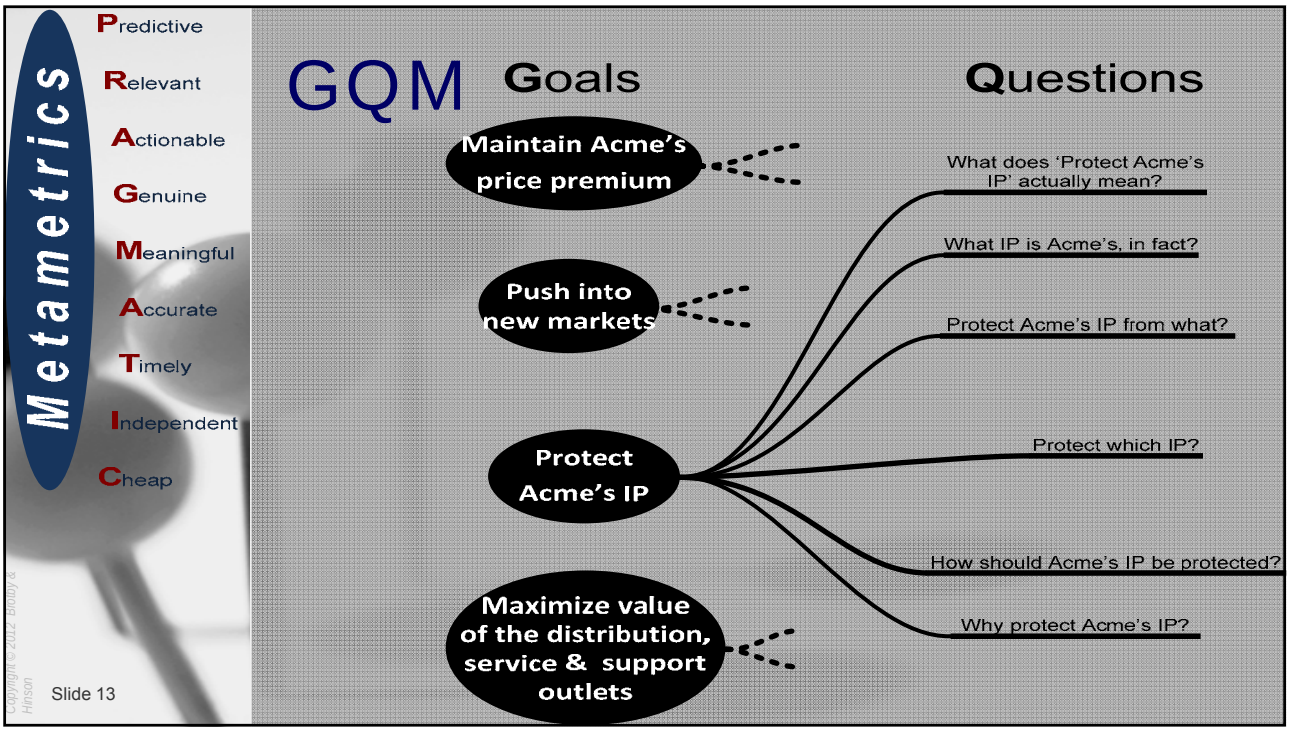
Slide 11

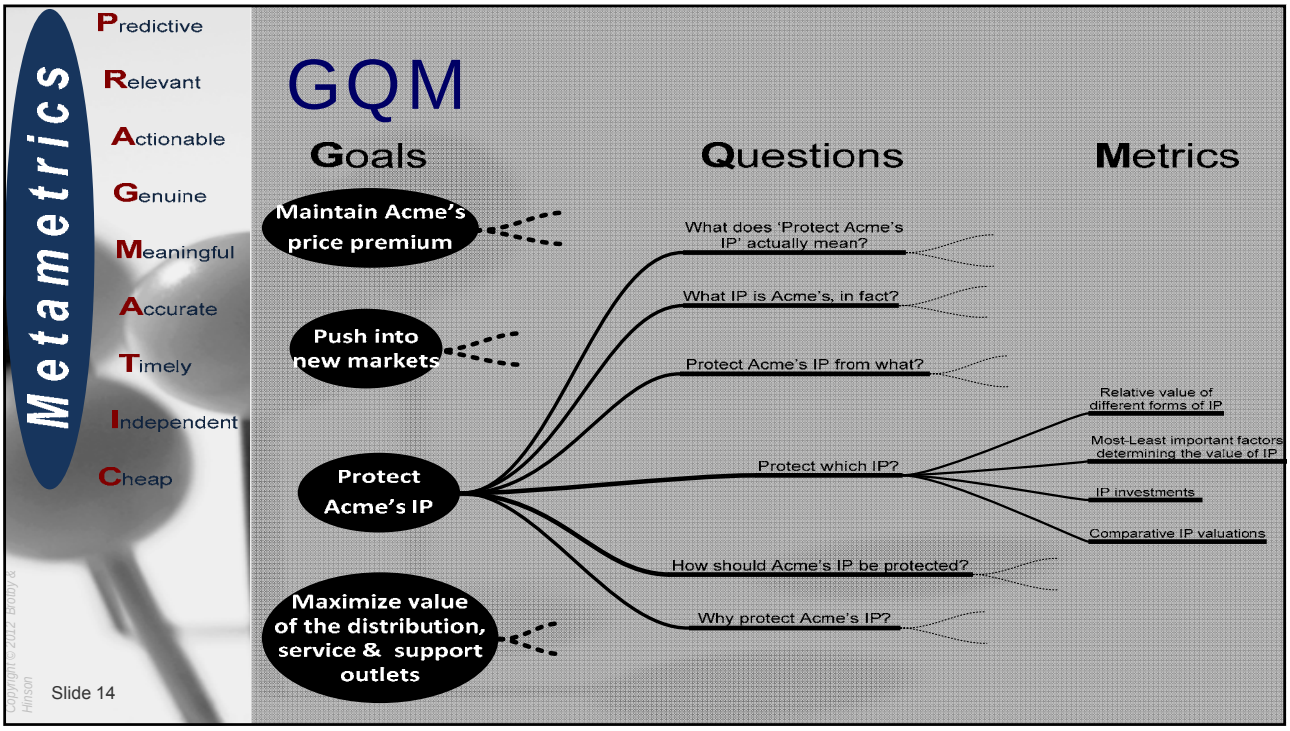
Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

GQM

Slide 12


Metametrics
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap
GQM
Goals
Questions
Maintain Acme's price premium
Push into new markets
Protect Acme's IP
Maximize value of the distribution, service & support outlets
What does 'Protect Acme's IP' actually mean?
What IP is Acme's, in fact?
Protect Acme's IP from what?
Protect which IP?
How should Acme's IP be protected?
Why protect Acme's IP?
Slide 13


Metametrics
Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap
GQM
Goals
Questions
Metrics
Maintain Acme's price premium
Push into new markets
Protect Acme's IP
Maximize value of the distribution, service & support outlets
What does 'Protect Acme's IP' actually mean?
What IP is Acme's, in fact?
Protect Acme's IP from what?
Protect which IP?
How should Acme's IP be protected?
Why protect Acme's IP?
Relative value of different forms of IP
Most-Least important factors determining the value of IP
IP investments
Comparative IP valuations
Slide 14

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Half a dozen dials …

"Every CSO should have half a dozen dials to watch on a regular basis. These indicators could be 'survival metrics,' the hot buttons on a dashboard you are expected to address that monitor the wellness of your organization or an issue of particular concern to management."

George K. Campbell

Slide 15

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Metametrics

- Uptime
- Failed logons
- Malware detected
- Vulnerabilities identified
- Dropped packets
- Unpatched systems

Slide 16

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

SMART metrics

There is no clear consensus about what the five or seven keywords mean, or even what they are in any given situation. Typically accepted values are:

Letter	Major Term	Minor Terms
S	Specific	Significant, Stretching, Simple
M	Measurable	Meaningful, Motivational, Manageable
A	Attainable	Appropriate, Achievable, Agreed, Assignable, Actionable, Ambitious, Aligned, Aspirational, Acceptable, Action-focused
R	Relevant	Results-oriented, Realistic, Resourced, Resonant
T	Timely	Time-oriented, Time framed, Timed, Time-based, Timeboxed, Time-bound, Time-Specific, Timetabled, Time limited, Trackable, Tangible
E	Evaluate	Ethical, Excitable, Enjoyable, Engaging, Ecological
R	Reevaluate	Rewarded, Reassess, Revisit, Recordable, Rewarding, Reaching

Table from Wikipedia

SMART attributed to Paul J. Meyer

Slide 17

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

PRAGMATIC

Metametrics

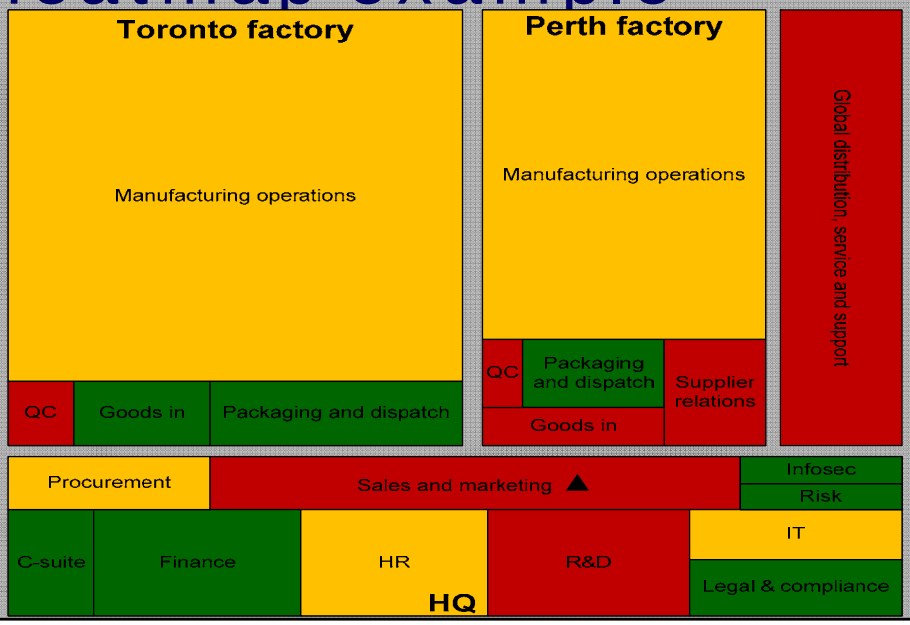
Predictive – forward-looking
Relevant – to the business and infosec
Actionable – controllable, do-able
Genuine – can't be faked or falsified
Meaningful – to the audience
Accurate – enough to be useful
Timely – here and now
Independent – hence verifiable
Cheap – always a bonus!

Slide 18

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Heatmap example



Slide 19

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Drilling down

Sales and Marketing infosec status, May 2012:

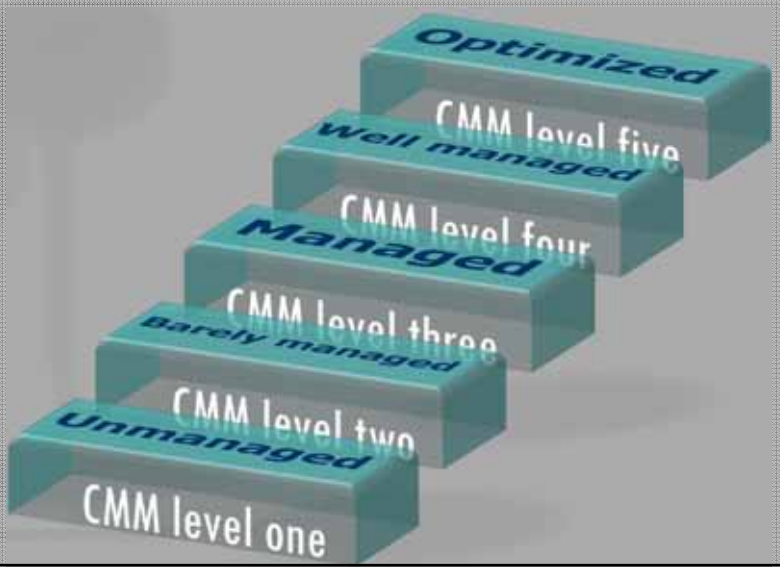
69%	Risk management
79%	Policy ▲
61%	Organization
44%	Asset management
20%	HR security
31%	Physical & environmental
58%	Comms & ops management
58%	Access control ▲
69%	Software development
73%	Incident management
10%	Business continuity ▼
39%	Compliance
51%	**OVERALL**

Slide 20

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Classic CMM



Slide 21

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Scoring scales

ISO/IEC 27002 section 8: human resources security maturity metrics

0% 33% 66% 100%

No human resources security	Basic human resources security	Good human resources security	Excellent human resources security
Information security rôles and responsibilities are entirely undocumented	Some information security rôles and responsibilities are documented, though not very well or consistently	Most information security rôles and responsibilities, including all the important ones, are assigned to individuals through being incorporated into vacancy notices, job descriptions and/or codes of conduct	Information security rôles and responsibilities are comprehensively documented, formally assigned to suitable individuals (typically in legally-binding contracts of employment or terms and conditions of employment), and are proactively maintained (e.g. periodically reconfirmed with the individual's signature to confirm their acceptance)
It does not even occur to management that candidates and employees might not be entirely	New employees may be security screened where the rôles are obviously sensitive or trusted, but the processes are weak and inconsistent; most	New employees are routinely security screened prior to employment, especially for sensitive or trusted rôles, using a documented screening process or background checks such as taking up	Prospective employees are routinely security screened, background checked or positively vetted according to the nature of the rôles, prior

Slide 22

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Pragmatic scoring

Criterion	Rating guide 0%	33%	66%	100%
PREDICTIVE	The metric is purely historical and backward-looking, with no predictive value whatsoever	Principally historic but gives some vague indication of the future direction such as weak trends	Definitely has predictive value such as strong trends, but some doubt and apparently random variability remains	Highly predictive, unambiguously indicative of future conditions with very strong cause-and-effect linkages
RELEVANT	The metric is totally irrelevant to information security	The metric has marginal relevance to information security, with narrow application or some irrelevant aspects	The metric is quite relevant to information security, but there are a few exceptions or drawbacks	The metric is absolutely relevant to information security
ACTIONABLE	Recipients have absolutely no idea what to do with this	The metric vaguely hints at what needs to be done,	The metric gives a very good steer on what needs to be done and would	The metric is proscriptive, directly actionable and would definitely

Slide 23

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Scoring a heat map

Example security metric 14.9
Mapping critical business processes to disaster recovery and business continuity plans

P	R	A	G	M	A	T	I	C	Score
85	92	79	81	90	70	75	40	40	72%

Here we envisage some sort of physical overlay on the business process landscape/map noted earlier, showing both the extent to which DR and BC arrangements cover the landscape, and the status of those arrangements, particularly in relation to the most critical business processes. A heat map might for instance indicate areas that have achieved a complete pass (green), a partial fail (yellow), or a severe fail, untested or unspecified (red), in each case comparing the resilience and recovery test results achieved against the corresponding business continuity requirements as specified by the Information Asset Owners. Further details could be provided to substantiate the reported values, for example business continuity sign-offs from the Information Asset Owners for the greens, allocated action plans for the yellows, and for the reds either proposals to address them or at least statements identifying the people responsible for developing the proposals. Provided it is carefully defined and applied, reporting on DR/BC arrangements that are 'suitable' would give senior management a more strategic overview of the organization's BC status. With a bit more sophistication, this metric could be turned into a process maturity metric, distinguishing systems/processes where the business continuity requirements are merely 'defined', from those which are 'defined and in place', and ultimately from those which are 'defined, in place and proven'. A single "percentage covered" number would be simpler to report but would have much less impact and value to the recipients, since it would lack those vital details about which processes or areas remain exposed.

Slide 24

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

A metrics catalog

Rank	Reference	Example metric	Strategic, Managerial or Operational	PRAGMATIC ratings (percent)									Score
				Predictive	Relevant	Actionable	Genuine	Meaningful	Accurate	Timely	Independent	Cost	
39	7.4	Unowned information asset days	M O	40	51	84	77	74	86	92	94	82	76%
40	14.8	IT capacity and performance	S M O	92	92	82	77	96	62	84	64	29	75%
41	5.7	Number or % of security policies addressing viable risks	M	65	76	91	73	83	77	70	61	78	75%
42	9.4	Number of unsecured access points	M O	95	80	90	70	85	77	45	75	55	75%
43	13.2	Time taken to remediate security incidents	M	82	69	85	76	80	75	65	75	60	74%
44	15.4	Status of compliance with externally-imposed information security obligations	S M O	77	85	85	70	98	68	35	89	60	74%
45	12.3	Software quality assurance	M	83	85	91	73	90	68	70	80	20	73%
46	5.8	Quality of security policies	M O	80	85	40	66	72	75	80	80	80	73%
47	12.4	Quality of system security revealed by testing	M	83	88	83	73	90	68	80	82	10	73%
48	10.3	Time from change approval to change	M	70	71	76	90	60	84	64	60	80	73%
49	10.4	Correlation between system/configuration logs and authorized change requests	M	87	80	90	80	80	80	60	50	47	73%
50	14.9	Mapping critical business processes to disaster recovery and business continuity plans	S M	85	92	79	81	90	70	75	40	40	72%
51	5.10	Thud factor (policy verbosity/red tape index, waffle-o-meter)	M	82	80	60	60	70	45	85	86	84	72%
52	5.9	% of policy statements unambiguously	M	92	91	64	60	85	65	45	75	75	72%

Slide 25

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Advanced metametrics

- Weighting the PRAGMATIC criteria
- Compiling, ranking, sharing & comparing metrics catalogs
- Creative measures: more for less
- Information security metrics *system*
- Measure *anything*

Slide 26

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Electronic Mail System

From: InformationSecurityManager@AcmeEntInc.com
To: ChiefExecutiveOfficer@AcmeEngInc.com
Subject: Information security budget

Dear Fred,

Thank you for the opportunity to explain the basis for the information security budget. As I'm sure you know, we have been quietly developing an information security measurement system comprising a suite of security metrics addressing the very issues you raise, so I hope the following information is exactly what you need.

1. **Return on investment**: the original business case for the Information Security Management System laid out the projected costs and benefits in order to justify both the initial investment and the ongoing operations. We have been diligently tracking actuals against the plan for the eighteen months since we got the green light for the ISMS. I am delighted to report that although the project consumed all its contingency, the returns have thus far exceeded our expectations **(exhibit 1)**:

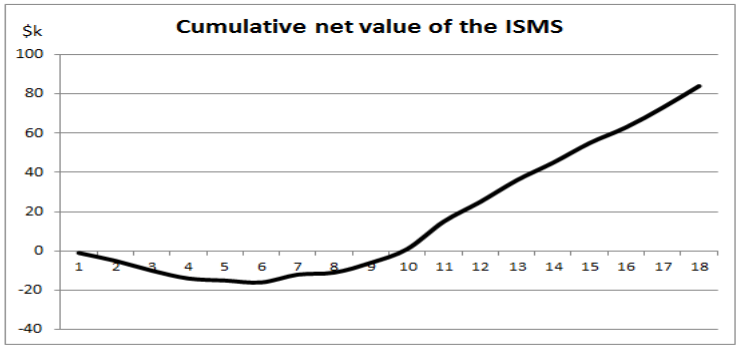


Exhibit 1: Net value of the Information Security Management System

Slide 27

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

A substantial saving was made by identifying and eliminating approximately 15% of our outdated information security controls without, of course, a corresponding increase in risk. With assistance from Finance, we are accounting for the savings on a decreasing basis over five years, and we have instituted a regular controls review process to release further savings.

2. **Security benchmarking**: although we are not yet confident enough to benchmark Acme against our industry peers, we have been steadily developing our capabilities through internal benchmarking, assessing the main business units against the ISO27k international security standards and comparing them against each other **(exhibit 2)**:

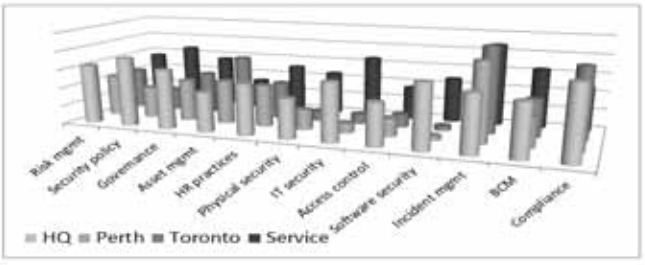


Exhibit 2 Security benchmarking

Thus far, we have identified a number of opportunities and launched three security improvement initiatives covering IT security, access control and software security at the factories. We are pleased to note the transfer of good practices between the business units in these three areas, and we plan to extend the concept once the initiatives near completion in 2 to 3 months.

3. **Potential security savings**: maintaining information security risks within acceptable limits is the key to keeping information security expenditure in check. Information Asset Owners (IAOs) throughout the business are accountable for adequately protecting their assets, so they are in the driving seat making management decisions on the controls they deem necessary, albeit under guidance from Risk Management and Information Security Management. At a broader level, senior managers are responsible for defining risk management and risk assessment methods and the risk appetite. The current 'top five' list shows how information security risks stack up in relation to other risks.
   1. Commercial/market risk due to Far Eastern competition
   2. Theft of Acme intellectual property
   3. Compliance failures causing loss of ability to process credit cards
   4. Reputational damage, brand devaluation
   5. Cloud computing incident causing loss of IT services

Slide 28

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

If, as you imply, the information security risks are not at the appropriate level in the list, we would have to work with the IAOs to find ways to reduce the security protecting their assets and accept higher risks. For our own part, we have identified a few areas in which we believe we may be able to improve our efficiency and cost effectiveness and realize substantial savings over 5 years (**exhibit 3**):

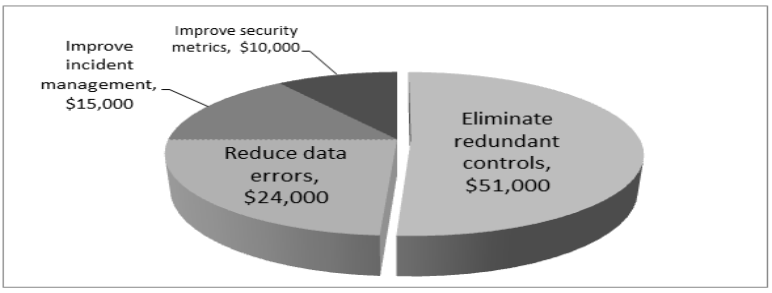


Exhibit 3: Estimated security savings over 5 years

As you will see from the data above, we are consciously taking a pragmatic, focused approach to the security metrics we use operationally and for security management, plus those of a more strategic nature that are reported to senior management.

Please let me know if you would like to discuss the meaning and/or the way we present the metrics as we would like to incorporate this kind of information into our regular management reports, and we don't want to waste your time with irrelevancies. Given the chance, I would love to help you prepare and perhaps deliver a briefing to the Board demonstrating how much we are achieving for the business through our professional, good practice approach to information security.

Regards,

John D,

Information Security Manager

Slide 29

Metametrics

Predictive
Relevant
Actionable
Genuine
Meaningful
Accurate
Timely
Independent
Cheap

Join the discussion

Slide 30